Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

Long-distance quantum key distribution using concatenated entanglement swapping with practical resources

Aeysha Khalique
Barry C. Sanders

SPIE.

Aeysha Khalique, Barry C. Sanders, "Long-distance quantum key distribution using concatenated entanglement swapping with practical resources," *Opt. Eng.* **56**(1), 016114 (2017), doi: 10.1117/1.OE.56.1.016114.

Long-distance quantum key distribution using concatenated entanglement swapping with practical resources

Aeysha Khalique[a,b,c,*] **and Barry C. Sanders**[b,c,d,e,f]
[a]National University of Sciences and Technology, School of Natural Sciences, H-12 Islamabad, Pakistan
[b]University of Science and Technology of China, Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai, China
[c]University of Science and Technology of China, Hefei National Laboratory for Physical Sciences at Microscale, Hefei, Anhui, China
[d]University of Calgary, Institute for Quantum Science and Technology, Alberta, Canada
[e]Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California, United States
[f]Canadian Institute for Advanced Research, Program in Quantum Information Science, Toronto, Ontario, Canada

Abstract. We explain how to share photons between two distant parties using concatenated entanglement swapping and assess performance according to the two-photon visibility as the figure of merit. From this analysis, we readily see the key generation rate and the quantum bit error rate as figures of merit for this scheme applied to quantum key distribution (QKD). Our model accounts for practical limitations, including higher-order photon pair events, dark counts, detector inefficiency, and photon losses. Our analysis shows that compromises are needed among the runtimes for the experiment, the rate of producing photon pairs, and the choice of detector efficiency. From our quantitative results, we observe that concatenated entanglement swapping enables secure QKD over long distances but at key generation rates that are far too low to be useful for large separations. We find that the key generation rates are close to both the Takeoka–Guha–Wilde and the Pirandola–Laurenza–Ottaviani–Banchi bounds. [DOI: 10.1117/1.OE.56.1.016114]

Keywords: quantum key distribution; entanglement swapping; long-distance quantum communication.

Paper 161639P received Oct. 20, 2016; accepted for publication Jan. 5, 2017; published online Jan. 25, 2017.

1 Introduction

Quantum communication provides a means for secure communication in open channels.[1] One of the primary goals of quantum communication is to develop the ability to communicate at arbitrary distances. Experimentally, communication distances have been limited to a few 100 km. Recently, quantum key distribution (QKD) of up to 200 km has been achieved with measurement-device-independent QKD.[2] A distance of up to 250 km has been achieved using a subcarrier wave modulation method, which employs the Bennett–Brassard protocol.[3] Quantum relays and repeaters are promising setups to achieve the ultimate goal of long-distance quantum communication.[4] In principle, any distance is achievable using quantum relays. In practice, however, the allowed distance is limited by resource imperfections. These imperfections also limit the key generation rate, which will affect the efficacy of the system.

Quantum relays and repeaters have been investigated for long-distance key distribution[5] which models the resources with approximations. We provide a rigorous model for a quantum relay setup based on entanglement swapping in which we have included the imperfections of the sources, the channels, and the detectors.[6,7] This concatenated entanglement swapping setup is then extended to key distribution protocol,[8] which relies on the Bennett–Brassard–Mermin[9] protocol. In this paper, we explain our approach to model concatenated entanglement swapping and key distribution protocol based on such a swapping setup.[10] Our approach could be useful for modeling long-distance quantum communication incorporating quantum memories and by extension quantum repeaters.

This paper is organized as follows: in Sec. 2, we explain the entanglement swapping process and discuss the resources proposed for an experimental setup. In Sec. 3, we present the model for a single swap and calculation of four-photon visibility based on that. The concatenated entanglement swapping setup for long-distance quantum communication and the corresponding results for visibility are shown in Sec. 4. In Sec. 5, we present the QKD protocol based on concatenated entanglement swapping and show the results for maximum key generation rates with optimized resource parameters. Finally, we conclude in Sec. 6.

2 Devices for Entanglement Swapping

The achievable distance in quantum communication can be increased by entanglement swapping. In this section, we briefly review the entanglement swapping procedure and the devices used in a swapping experiment. We explain the entanglement swapping procedure in Sec. 2.1 and the practical devices in Sec. 2.2.

2.1 *Entanglement Swapping with Perfect Devices*

Entanglement swapping provides a means for entangling distant parties who have never interacted in the past. Figure 1 shows the entanglement of possibly distant parties A and B,

*Address all correspondence to: Aeysha Khalique, E-mail: ashkhalique@gmail.com

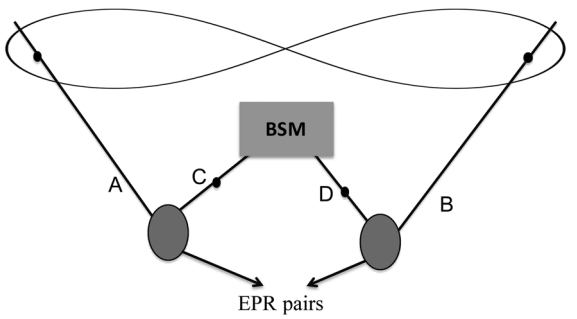

Fig. 1 Two Einstein–Podolsky–Rosen (EPR) sources produce entangled pairs AC and BD. A BSM on C and D entangles A and B.

when their entangled partners, C and D, undergo a Bell-state measurement (BSM). BSM distinguishes between the four Bell states

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|\mathrm{HV}\rangle + |\mathrm{VH}\rangle);$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\mathrm{HV}\rangle - |\mathrm{VH}\rangle);$$
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\mathrm{HH}\rangle + |\mathrm{VV}\rangle); \quad \text{and}$$
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|\mathrm{HH}\rangle - |\mathrm{VV}\rangle), \tag{1}$$

Entanglement swapping is evident from the fact that the combined entangled state of AC and BD is

$$|\psi^+\rangle_{\mathrm{AC}}|\psi^+\rangle_{\mathrm{BD}} = \frac{1}{2}[|\psi^+\rangle_{\mathrm{AB}}|\psi^+\rangle_{\mathrm{CD}} + |\psi^-\rangle_{\mathrm{AB}}|\psi^-\rangle_{\mathrm{CD}} + |\phi^+\rangle_{\mathrm{AB}}|\phi^+\rangle_{\mathrm{CD}} + |\phi^-\rangle_{\mathrm{AB}}|\phi^-\rangle_{\mathrm{CD}}]. \tag{2}$$

Thus, BSM on C and D projects A and B into the corresponding Bell state.

2.2 *Resources*

In a typical entanglement swapping setup, the relevant resources are the entanglement source, the channels, and the detectors. All these resources have imperfections. For convenience, we list the definition of parameters used in this paper in Table 1.

First, we consider a parametric down-conversion (PDC) entanglement source that produces multipairs of entangled photons. The state of the photons entangled in horizontal–vertical (H–V) polarization is

$$|\chi\rangle = \mathrm{e}^{\mathrm{i}\chi\left(\hat{a}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger}+\mathrm{hc}\right)}|\mathrm{vac}\rangle = \mathrm{sech}^2\chi\mathrm{e}^{\mathrm{i}\tanh\chi\left(\hat{a}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger}\right)}|\mathrm{vac}\rangle, \tag{3}$$

where χ^2 is the multipair production rate of the source, and $\hat{a}_{\mathrm{H}}^{\dagger}$ and $\hat{c}_{\mathrm{H}}^{\dagger}$ are the creation operators for horizontally polarized photons in spatial modes A and C, respectively. The corresponding creation operators $\hat{a}_{\mathrm{V}}^{\dagger}$ and $\hat{c}_{\mathrm{V}}^{\dagger}$ are for vertically polarized photons.

We consider a fiber optic channel with distance-dependent loss coefficient α. The channel efficiency is

Table 1 Definition of various symbols for experimental parameters used in the paper.

Symbol	Definition
χ^2	Multipair production rate of the source
η_t	Channel efficiency
η_0	Intrinsic efficiency of detector
η	Total efficiency
$\wp$	Dark count rate of detector
α	Distance-dependent loss coefficient of the channel
α_0	Distance-independent loss coefficient of the setup
N	Number of entanglement swappings
δ_A	Angle of the polarization rotator at the left
δ_B	Angle of the polarization rotator at the right
ℓ	Communication distance

$$\eta_{\mathrm{t}} = \mathrm{e}^{-(\alpha\ell+\alpha_0)/10}, \tag{4}$$

where ℓ is the length of the fiber and α_0 is the distance-independent loss. The same model can be employed to model free-space transmission.

A realistic detector is modeled as pairing of a perfect detector with a beam splitter (BS)[11] as shown in Fig. 2. Both the detector's intrinsic efficiency η_0 and the channel transmission efficiency η_t are included in the transmission efficiency of the BS, which in turn is $\eta = \eta_0\eta_t$. The dark counts of the detector are modeled by a thermal source of light, which represents stray photons incident on one port of the BS. These photons, which are at pseudotemperature T, with T chosen as an adjustable parameter to model the detector, can be expressed by the state[11]

$$\hat{\rho}_T = (1 - \mathrm{e}^{-\hbar\omega/k_{\mathrm{B}}T})\sum_{n=0}^{\infty}\mathrm{e}^{-n\hbar\omega/k_{\mathrm{B}}T}|n\rangle\langle n|, \tag{5}$$

where $|n\rangle$ is the photon number state.

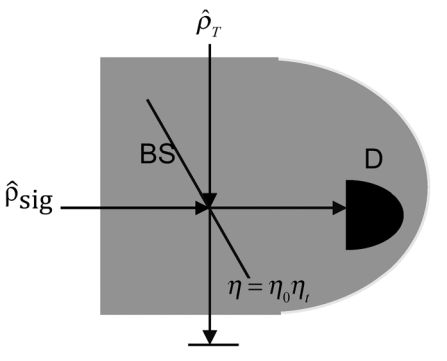

Fig. 2 The imperfect detector is represented by a BS and a perfect detector (D). A signal beam $\hat{\rho}_{\mathrm{sig}}$ is incident on one port, and thermal light $\hat{\rho}_{\mathrm{T}}$ is incident on the other port. The BS has efficiency η, which comprises the detector's intrinsic efficiency η_0, and the channel efficiency η_t.

The signal photons $\hat{\rho}_{\text{sig}}$ are incident on the other port. Threshold detectors have two possibilities, with $q = 0$ corresponding to no click and $q = 1$ corresponding to a click. The probability of detecting q photons given i incident photons is

$$P(q = 0|i) = (1 - \wp)[1 - \eta(1 - \wp)]^i = 1 - P(q = 1|i), \tag{6}$$

where i is the number of photons in the signal state $\hat{\rho}_{\text{sig}} = |i\rangle\langle i|$ and $\wp$ is the dark count probability. The detectors are mutually independent and the conditional probability of detecting q, r, s, and t photons, each on one of the four detectors for i, j, k, and l incident signal photons, respectively, is the following product of four independent probabilities:

$$P(qrst|ijkl) = P(q|i)P(r|j)P(s|k)P(t|l). \tag{7}$$

Now, we have a mathematical framework for each of the three pertinent devices, namely the sources, the channels, and the detectors.

3 Practical Single Swap: Coincidence Probabilities and Visibility

In practice, the entanglement swapping setup consists of two PDC sources. Figure 3 shows two parties A and B, which become entangled by BSM at the two inner ports. The BSM setup consists of a BS followed by polarization rotators and polarization BSs that separate the horizontal and vertical polarized photons. These photons are detected at the four photodetectors. The detector clicks corresponding to ideal BSM outcomes for various Bell states are given in Table 2.

The fourfold coincidence is the coincidence of detector clicks in spatial modes a_1 and d_1, shown in Fig. 3, given that the Bell measurement has resulted in the clicks (0101) or (1010) at the inner detectors. These clicks at the inner detectors correspond to the measurement of the Bell state $|\psi^+\rangle$ as shown in Table 2. Out of various coincidences, $(q'r's't') \in \{(0101), (1010)\}$ occurs a maximum number of times, and the probability of occurrence of these coincidences is the maximum coincidence probability

$$Q_{\max}(qrst) = \max_{q'r's't'} Q(q'r's't'|qrst;\chi,\wp,\eta), \tag{8}$$

where $Q_{\max}(qrst)$ depends on the resource parameters, χ, $\wp$, and η. The coincidences, $(q'r's't') \in \{(0110), (1001)\}$,

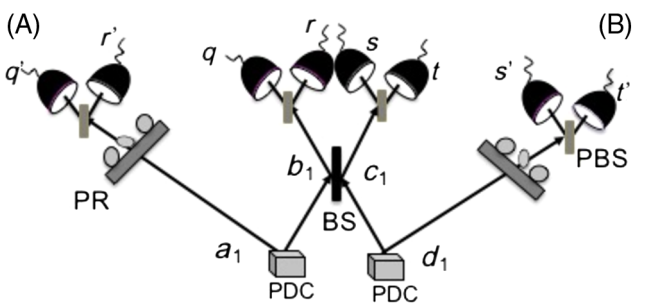

Fig. 3 Experimental setup for single swap. q' and r' represent the clicks on detectors at A, and s' and t' are clicks on those at B. q, r, s, and t are the clicks at inner detectors. PR labels a polarizer rotator, PBS labels a polarizing BS, and BS labels a BS. PDC labels a PDC source.

Table 2 Recorded clicks ($qrst$) on four detectors after the BSM, corresponding to the four Bell states $|\psi^{\pm}\rangle$ and $|\phi^{\pm}\rangle$.

State	($qrst$)
$\|\psi^+\rangle$	(1010) ∨ (0101)
$\|\psi^-\rangle$	(0110) ∨ (1001)
$\|\phi^{\pm}\rangle$	(2000) ∨ (0200) ∨ (0020) ∨ (0002)

occur for a minimum number of times, and the probability of occurrence of these coincidences is the minimum coincidence probability

$$Q_{\min}(qrst) = \min_{q'r's't'} Q(q'r's't'|qrst;\chi,\wp,\eta), \tag{9}$$

which also depends on the resource parameters, χ, $\wp$, and η. The degree of entanglement is then quantified using visibility

$$V(\chi,\wp,\eta) := \frac{Q_{\max} - Q_{\min}}{Q_{\max} + Q_{\min}}. \tag{10}$$

Conditional probability Q is calculated by the following course of action on the photons produced by the two PDCs.[12] The photons in the inner two channels undergo the action of BS U_{B} yielding

$$|\Xi\rangle = U_{\text{B}}|\chi\rangle_{\text{AC}}|\chi\rangle_{\text{BD}}, \tag{11}$$

and the ideal detection of photons i, j, k, and l at the inner detectors is reflected by Fock projection Π^{inn}_{ijkl}, which yields the state

$$|\tilde{\Xi}\rangle^{\text{out}}_{ijkl} := \frac{\langle ijkl|_{\text{CD}}\Pi^{\text{inn}}_{ijkl}|\Xi\rangle}{\sqrt{P(ijkl)}}, \tag{12}$$

at the outer ports. Here $P(ijkl) = \langle\Xi|\Pi^{\text{inn}}_{ijkl}|\Xi\rangle$. The noisy detection at the inner ports produces a mixed state,

$$\rho^{\text{out}}_{qrst} = \sum P(ijkl|qrst)|\tilde{\Xi}\rangle^{\text{out}}_{ijkl}\langle\tilde{\Xi}|, \tag{13}$$

at the outer ports. Here, $P(ijkl|qrst)$ is the conditional probability that $ijkl$ photons are detected ideally given actual detection $qrst$. This probability can be found from the known probability $P(qrst|ijkl)$ given in Eq. (7) using Bayes' theorem

$$\begin{aligned} P(ijkl|qrst) &= \frac{P(qrst|ijkl)P(ijkl)}{P(qrst)} \\ &= P(q|i)P(r|j)P(s|k)P(t|l)P(ijkl)/P(qrst). \end{aligned} \tag{14}$$

The conditional probability of detecting $i'j'k'l'$ photons at ideal outer detectors, given actual counts $qrst$ at the inner ones, after passing through the polarization rotators at angles δ_A and δ_B, is

$$P(i'j'k'l'|qrst) = \langle i'j'k'l'|U(\delta_A)U(\delta_B)\rho^{\text{out}}_{qrst}U^\dagger(\delta_A) \times U^\dagger(\delta_B)|i'j'k'l'\rangle. \quad (15)$$

The fourfold coincidence probability Q of detecting actual photons $q'r's't'$ at the outer four detectors given $qrst$ at the inner ones is

$$Q(q'r's't'|qrst) = \sum_{i'j'k'l'} P(q'r's't'|i'j'k'l';\wp,\eta) \times P(i'j'k'l'|qrst). \quad (16)$$

This expression for Q can thus be calculated using Eqs. (14) and (15).

4 Extending the Distance by Arbitrary Swaps

Communication distance can be extended by concatenating signal swaps. We analyze such a setup and calculate the corresponding visibility. We give a closed-form solution for calculation of $Q_{\text{ext}}(qrst)$ for an arbitrary number of swaps in Sec. 4.1. In Sec. 4.2, we give our results for calculation of visibility for $N \leq 3$.

4.1 *Closed-Form Solution for Calculation of $Q_{\text{ext}}(qrst)$ for N Swaps*

The configuration for concatenated N swaps is shown in Fig. 4. For N swaps, there are $2N-1$ BSMs. Ideally, successful BSM at the inner stations entangles distant parties A and B at the extreme ends. However, practically, the maximum probability of clicks at the outer detectors corresponding to clicks **qrst** at the inner ones is dependent on resource parameters χ, $\wp$, and η,

$$Q_{\text{ext}}(qrst) = \underset{q'r's't'}{\text{ext}} Q(q'r's't'|\mathbf{qrst};\chi,\wp,\eta), \quad (17)$$

where $\mathbf{q} = \{q_1, q_2, \ldots, q_{2\,N-1}\}$, and the same goes for **r**, **s**, and **t**.

The closed-form solution of the conditional probability $P(i'j'k'l'|\mathbf{qrst})$ is Ref. 7

$$\begin{aligned}
P(i'j'k'l'|\mathbf{qrst}) &= \sum_{\mathbf{ijkl}} P(\mathbf{ijkl}|\mathbf{qrst})\langle i'j'k'l'|U(\alpha)U(\delta)|\tilde{\Xi}\rangle^{\text{out}}_{\mathbf{ijkl}}\langle\tilde{\Xi}|U^\dagger(\alpha)U^\dagger(\delta)|i'j'k'l'\rangle \\
&= \sum_{\mathbf{ijkl}} \frac{P(\mathbf{qrst}|\mathbf{ijkl})}{P(\mathbf{qrst})}\left[\frac{1}{\sqrt{2^{i_1+j_1+k_1+l_1}i_1!j_1!k_1!l_1!}}\frac{(\tanh\chi)^{i_1+j_1+k_1+l_1}}{\cosh^{4\,N}\chi}\sum_{\mu_1=0}^{i_1}\sum_{\nu_1=0}^{j_1}\sum_{\kappa_1=0}^{k_1}\sum_{\lambda_1=0}^{l_1}(-1)^{\mu_1+\nu_1}\binom{i_1}{\mu_1}\binom{j_1}{\nu_1}\right. \\
&\times\binom{k_1}{\kappa_1}\binom{l_1}{\lambda_1}\cdots\frac{1}{\sqrt{2^{i_N+j_N+k_N+l_N}i_N!j_N!k_N!l_N!}}\frac{(\tanh\chi)^{i_N+j_N+k_N+l_N}}{\cosh^{4N}\chi} \\
&\times\left.\sum_{\mu_N=0}^{i_N}\sum_{\nu_N=0}^{j_N}\sum_{\kappa_N=0}^{k_N}\sum_{\lambda_N=0}^{l_N}(-1)^{\mu_N+\nu_N}\binom{i_p}{\mu_N}\binom{j_N}{\nu_N}\binom{k_N}{\kappa_N}\binom{l_N}{\lambda_N}\right] \\
&\times\prod_{n=1}^{N-1}\Omega(\mu_n,\lambda_n,i_{N+n},l_{N+n})\Omega(\nu_n,\kappa_n,j_{N+n},k_{N+n})\frac{\sqrt{i_{N+n}!j_{N+n}!k_{N+n}!l_{N+n}!}}{\sqrt{2}^{i_{N+n}+j_{N+n}+k_{N+n}+l_{N+n}}} \\
&\times(\nu_N+\kappa_N)!(j_1+k_1-\nu_1-\kappa_1)!\sqrt{\frac{j'!k'!}{i'!l'!}}\sum_{n_a=0}^{\min[j',\nu_N+\kappa_N]}\sum_{n_d=0}^{\min[k',j_1+k_1-\nu_1-\kappa_1]} \\
&\times\delta_{i_{N+n}+l_{N+n},\mu_n+\lambda_n+i_{n+1}+l_{n+1}-\mu_{n+1}-\lambda_{n+1}}\delta_{j_{N+n}+k_{N+n},\nu_n+\kappa_n+j_{n+1}+k_{n+1}-\nu_{n+1}-\kappa_{n+1}} \\
&\times\left(\text{i}\tan\frac{\delta_{\text{A}}}{2}\right)^{\nu_N+\kappa_N+j'-2n_a}\left(\cos\frac{\delta_{\text{A}}}{2}\right)^{i'+j'-2n_a}\left(\text{i}\tan\frac{\delta_{\text{B}}}{2}\right)^{k'+j_1+k_1-\nu_1-\kappa_1-2n_d}\left(\cos\frac{\delta_{\text{B}}}{2}\right)^{l'+k'-2n_d} \\
&\times\frac{(i'+j'-n_a)!(l'+k'-nd)!}{n_a!n_d!(j'-n_a)!(k'-n_d)!(\nu_N+\kappa_N-n_a)!(j_1+k_1-\nu_1-\kappa_1-n_d)!} \\
&\times\delta_{i'+j',\mu_N+\nu_N+\kappa_N+\lambda_N}\delta_{k'+l',i_1+j_1+k_1+l_1-\mu_1-\nu_1-\kappa_1-\lambda_1}. \quad (18)
\end{aligned}$$

Here

$$\Omega(\mu_n,\lambda_n,i_{N+n},l_{N+n}) = \sum_{\gamma=0}^{\mu_n+\lambda_n}\binom{\mu_n+\lambda_n}{\gamma} \times\binom{i_{N+n}+l_{N+n}-\mu_n-\lambda_n}{i_{N+n}-\gamma}(-1)^{\mu_n+\lambda_n-\gamma} \quad (19)$$

is the factor resulting from the BSM connecting the adjacent swaps.

4.2 *Visibility for $N \leq 3$ Swaps*

Here, we present our results for visibility and compare the same for $N = 1, 2$, and 3 concatenated swaps.[7] In Fig. 5, we give the coincidence probability $Q_{\max}(qrst) = Q(1010|1010) + Q(0101|1010)$ and $Q_{\min}(qrst) = Q(1001|1010) + Q(0110|1010)$ for varying δ_B. The visibility calculated from the curve at $\delta_B = \pm\pi/2$ is 16%. Visibility is compared for $N = 1, 2$, and 3 swaps in Fig. 6.

The communication distance increases as the number of concatenations increases. Figure 7 shows the comparison of

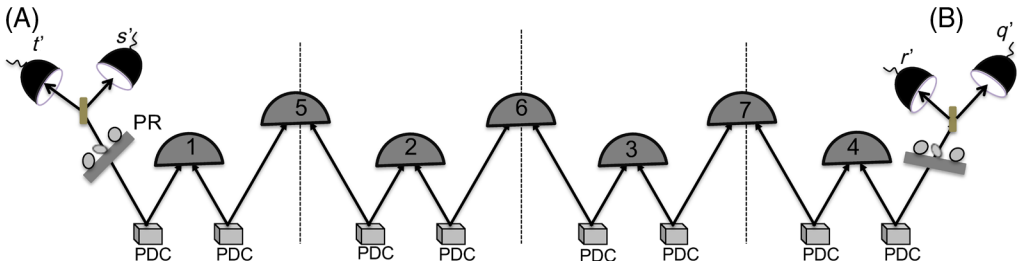

Fig. 4 Setup for concatenated entanglement swappings. For four concatenated swaps, seven BSMs at the inner stations entangle A and B at the two outer ends.

visibility for $N = 1, 2$, and 3 for various distances. The achievable distance increases to more than 1000 km for $N = 3$, but at the expense of very low visibility. The increase in distance tends to saturate as the number of concatenations increases. The rapid fall-off in visibility and limiting distance are due to detector dark counts and inefficiencies. For perfect detectors with $\eta_0 = 1$ and $\wp = 1$, an asymptotically large distance is achievable as shown in Fig. 8.

5 Long-Distance Quantum Key Distribution Protocol

The concatenated entanglement swapping setup described above is implemented in long-distance QKD protocol.[8] The setup is shown in Fig. 9. Two distant users A and B are

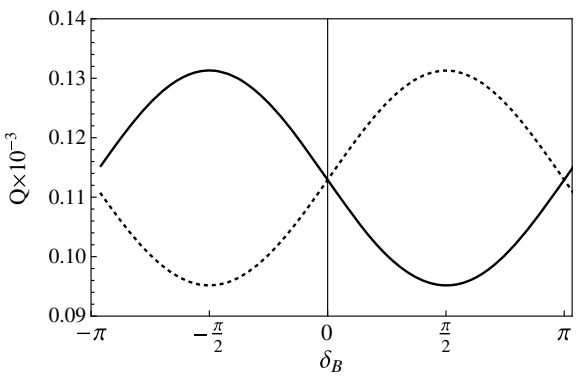

Fig. 5 $Q_{\text{max}}(qrst)$ (dotted curve) and $Q_{\text{min}}(qrst)$ (solid curve) are plotted versus δ_B for $\chi = 0.24$, $\eta = 0.04$, $\wp = 1 \times 10^{-5}$, and $\delta_A = \pi/2$. Figure reproduced from Fig. 4 of Khalique and Sanders.[7]

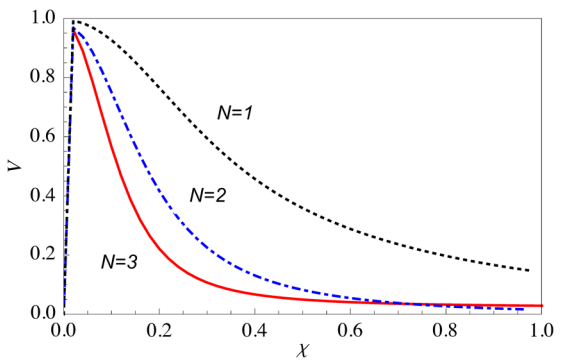

Fig. 6 Visibility is compared for $N = 1$, 2, and 3 for varying χ. Here, $\eta = 0.04$, $\wp = 1 \times 10^{-5}$, and $\delta_A = \delta_B = \pi/2$. Figure reproduced from Fig. 6 of Khalique and Sanders.[7]

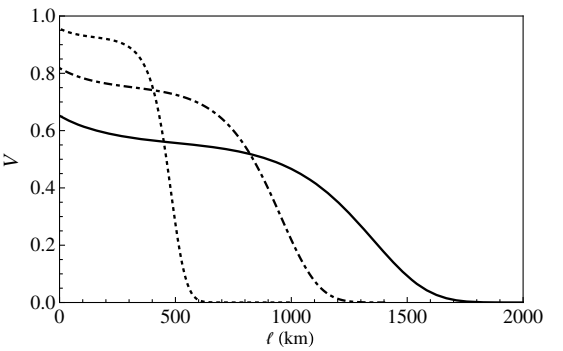

Fig. 7 Visibility is compared for $N = 1$ (dotted curve), $N = 2$ (dot-dashed curve), and $N = 3$ (solid curve) for various distances ℓ. Here, $\chi = 0.1$, $\eta_0 = 0.70$, $\wp = 1 \times 10^{-5}$, $\delta_A = \delta_B = \pi/2$, $\alpha = 0.25$ dB/km, and $\alpha_0 = 4$ dB. Figure reproduced from Fig. 6 of Khalique and Sanders.[7]

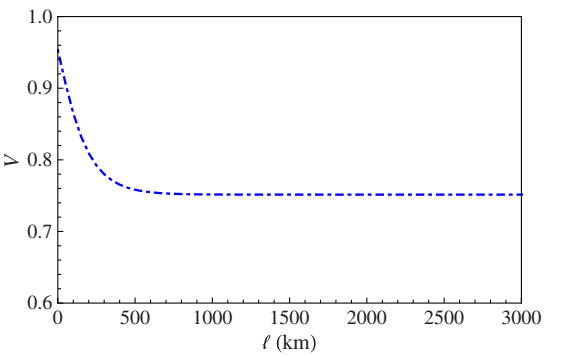

Fig. 8 Visibility V versus distance ℓ is shown for perfect detectors with $\eta_0 = 1$ and $\wp = 0$ for $N = 2$. Here, $\chi = 0.1$, $\delta_A = \delta_B = \pi/2$, $\alpha = 0.25$ dB/km, and $\alpha_0 = 0$ dB.

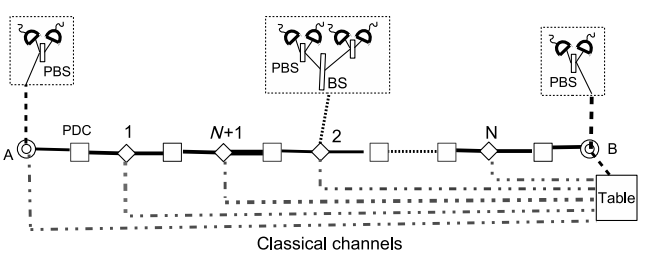

Fig. 9 Long-distance QKD setup is shown between users A and B. □ represents PDC source, and ⋄ represents the BSM setup. Figure reproduced from Fig. 1 of Khalique and Sanders.[8]

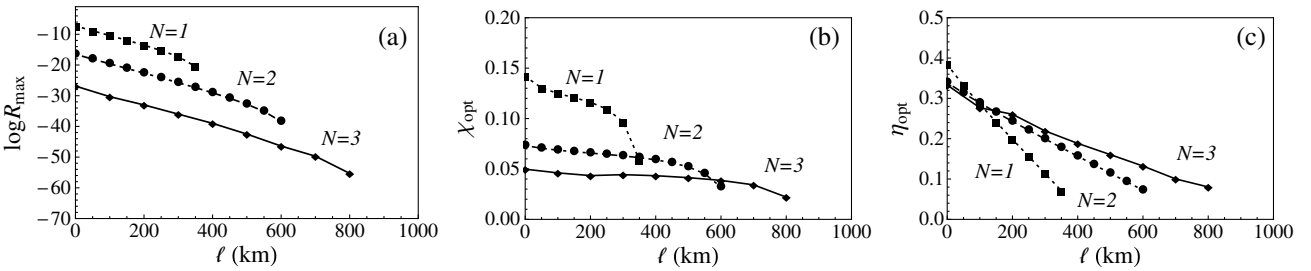

Fig. 10 (a) Plot of log R_{max} versus distance ℓ for $N = 1, 2$, and 3. (b) Corresponding optimal χ_{opt} is shown, and (c) optimal efficiency η_{opt} is shown. Here $\alpha = 0.25$ dB/km and $\alpha_0 = 4$ dB. Figure reproduced from Fig. 3 of Khalique and Sanders.[8]

connected by the concatenated entanglement swapping setup. Bell-state measurements at the intermediate stations ensure entanglement at the two extreme ends. The results of two-photon coincidence at the intermediate stations are sent to B, who calculates the visibility using these results and the two-photon coincidence at his and A's stations by the formalism developed for concatenated swapping. The visibility is related to the quantum bit error rate (QBER)[1]

$$\mathrm{QBER} = \frac{1-V}{2}. \tag{20}$$

The key generation rate is

$$R = R_{\mathrm{Shor-Preskill}} R_{\mathrm{sifted}}. \tag{21}$$

Here R comprises the sifted key rate

$$R_{\mathrm{sifted}} = \frac{1}{2}(\chi^2)^{2N} 10^{(-\alpha\ell/40\ N)4N} (\eta^2/2)^{2N-1}\eta^2, \tag{22}$$

and the key retained after error correction and privacy amplification

$$R_{\mathrm{Shor-Preskill}} = 1 - \kappa H_2(Q) - H_2(Q), \tag{23}$$

where κ is the reconciliation efficiency, with $\kappa = 1$ for perfect reconciliation. The net key rate is the product of the two rates. The linear-optical BSM process employed here is probabilistically bounded by its maximum value of 1/2,[13] which leads to a factor of $\eta^2/2$ in R_{sifted} in Eq. (22). Deterministic BSM, however, can be done using hyperentanglement,[14,15] which will require a source entangled in more than one degree of freedom.

We present the results obtained for maximized key generation rates R_{max} with optimum χ, η_0, and $\wp$[8] in Fig. 10. There is a trade-off between η_0 and $\wp$, as for very high efficiency, the contribution of dark counts in detected photons also increases, which lowers the visibility. We have used the trade-off corresponding to commonly used InGaAs detectors with

$$\wp = A\ \exp(B\eta_0), \tag{24}$$

where typically $A = 6.1 \times 10^{-7}$ and $B = 17$.[16]

Maximum key generation rates R_{max} and the optimal χ and η are shown in Fig. 10. Distances up to 850 km are achievable for $N = 3$, but at the cost of a very low key generation rate. We check the upper bound of the key generation rate and compare it with the Takeoka–Guha–Wilde (TGW) bound[17] and a more recent tighter Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound.[18] The TGW bound gives an upper bound on the key generation rate for nonrepeater-based QKD, which is

$$R_{\mathrm{TGW}} = \log_2\left(\frac{1+10^{-\alpha\ell/10}}{1-10^{-\alpha\ell/10}}\right), \tag{25}$$

and the PLOB bound for lossy channel is

$$R_{\mathrm{PLOB}} = \log_2\left(\frac{1}{1-10^{-\alpha\ell/10}}\right). \tag{26}$$

The upper bound for the concatenated entanglement swapping setup is calculated by setting $R_{\mathrm{Shor-Preskill}} = 1$ thus, $R = R_{\mathrm{sifted}}$. The comparison in Fig. 11 shows that the concatenated entanglement swapping key rates are close to the TGW and PLOB bound. Thus, quantum memories are needed to further increase the key generation rates resulting from concatenated entanglement swapping setup.

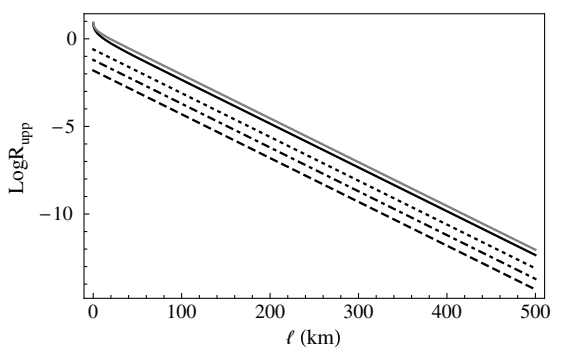

Fig. 11 Comparison between R_{TGW} bound (top most curve) R_{PLOB} (solid black curve) and upper bound of key rate for concatenated entanglement swapping for $N = 1$ (dotted curve), $N = 2$ (dot-dashed curve), and $N = 3$ (dashed curve).

6 Conclusions

We have presented our approach for calculation of visibility between distant parties using concatenated entanglement swapping with an arbitrary number of swaps and its application to long-distance QKD.[6–8] Our model incorporates the practical resources. The results show that large distances can be achieved by concatenated entanglement swapping, but this increase comes at the expense of atrociously low key generation rates. A trade-off is needed between experiment runtime, resource parameters, and key generation rates.

Acknowledgments

We thank Wolfgang Tittel, Michael Lamoreux, Artur Scherer, Norbert Lütkenhaus, and Pengqing Zhang for valuable discussions. BCS appreciates financial support provided by NSERC, Alberta Innovates Technology Futures, China's 1000 Talent Plan, and by the Institute for Quantum Information and Matter, which is a National Science Foundation Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-2644). This research has been enabled by the use of computing resources provided by WestGrid and Compute/Calcul Canada.

References

1. N. Gisin et al., "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145–195 (2002).
2. Y.-L. Tang et al., "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.* **113**, 190501 (2014).
3. A. V. Gleim et al., "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference," *Opt. Express* **24**(3), 2619 (2016).
4. N. Gisin and R. Thew, "Quantum communication," *Nat. Photonics* **1**(3), 165–171 (2007).
5. H. Krovi et al., "Practical quantum repeaters with parametric down-conversion sources," *Appl. Phys. B* **122**(3), 1 (2016).
6. A. Khalique, W. Tittel, and B. C. Sanders, "Practical long-distance quantum communication using concatenated entanglement swapping," *Phys. Rev. A* **88**, 022336 (2013).
7. A. Khalique and B. C. Sanders, "Long-distance quantum communication through any number of entanglement-swapping operations," *Phys. Rev. A* **90**, 032304 (2014).
8. A. Khalique and B. C. Sanders, "Practical long-distance quantum key distribution through concatenated entanglement swapping with parametric down-conversion sources," *J. Opt. Soc. Am. B* **32**(11), 2382 (2015).
9. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.* **68**, 557–559 (1992).
10. A. Khalique and B. C. Sanders, "Long-distance quantum-key-distribution using concatenated entanglement swapping with practical resources," *Proc. SPIE* **9980**, 99800R (2016).
11. P. P. Rohde and T. C. Ralph, "Modelling photo-detectors in quantum optics," *J. Mod. Opt.* **53**(11), 1589–1603 (2006).
12. A. Scherer et al., "Quantum states prepared by realistic entanglement swapping," *Phys. Rev. A* **80**, 062310 (2009).
13. J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical Bell-state analyzer," *Appl. Phys. B* **72**(1), 67–71 (2001).
14. C. Schuck et al., "Complete deterministic linear optics bell state analysis," *Phys. Rev. Lett.* **96**, 190501 (2006).
15. T.-C. Wei, J. T. Barreiro, and P. G. Kwiat, "Hyperentangled bell-state analysis," *Phys. Rev. A* **75**, 060305 (2007).
16. D. Collins, N. Gisin, and H. de Riedmatten, "Quantum relays for long distance quantum cryptography," *J. Mod. Opt.* **52**(5), 735–753 (2005).
17. M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nat. Commun.* **5**, 5235 (2014).
18. S. Pirandola et al., "Fundamental limits of repeaterless quantum communications," arXiv:1510.08863 (2015).

Aeysha Khalique received her doctorate in physics from Technische Universitat Darmstadt, Germany. She is head of the physics department at the School of Natural Sciences at National University of Sciences and Technology, Islamabad, Pakistan. She is currently managing the quantum information group at the University of Sciences and Technology Islamabad.

Barry C. Sanders is AITF iCORE strategic chair in quantum information science and director of the Institute for Quantum Science and Technology at the University of Calgary. He holds a 1000-Talents Chair at the University of Science and Technology of China. He is editor-in-chief of *New Journal of Physics* and fellow of the Institute of Physics (U.K.), the Optical Society of America, and the American Physical Society, and recently received an Imperial College London Doctor of Science degree.